

PRIMITIVE CENTRAL IDEMPOTENTS AND THE WEDDERBURN DECOMPOSITION OF A RATIONAL ABELIAN GROUP ALGEBRA

RAVI S. KULKARNI AND SOHAM S. PRADHAN

ABSTRACT. In this paper we give an explicit description of primitive central idempotents of rational group algebras of finite abelian groups using *long presentation*, and determine their Wedderburn decompositions.

Key Words: primitive central idempotent; group algebra; *long presentation*; Wedderburn decomposition.

1. INTRODUCTION

The classical approach of computing primitive central idempotents of a rational abelian group algebra $\mathbb{Q}[G]$, is to first compute the primitive central idempotents

$$e(\chi) = \frac{\chi(1)}{|G|} \sum_{g \in G} \chi(g^{-1})g$$

of $\mathbb{C}[G]$ associated with complex irreducible characters χ , and then sum the primitive central idempotents $e(\sigma\chi)$ with $\sigma \in \text{Gal}(\mathbb{Q}(\chi)/\mathbb{Q})$ to obtain the associated rational primitive central idempotent

$$e_{\mathbb{Q}}(\chi) = \sum_{\sigma \in \text{Gal}(\mathbb{Q}(\chi)/\mathbb{Q})} \sigma(e(\chi)).$$

An explicit description of primitive central idempotents of rational group algebra of a finite abelian group using subgroups structure was considered by several authors (see Ayoub [1], Theorem 5, Milies[2], Theorem 1.4, Jespers[3], Theorem 1.3). In this paper, we aim to give another explicit description of primitive central idempotents rational group algebra of a finite abelian group using *long presentation*.

It is a known fact that every primitive central idempotent of rational group algebra of a finite abelian group is product of primitive central idempotents of its p -primary parts, p a prime. This result brings our attention on the problem of computing primitive central idempotents of rational group algebra of a finite abelian p -group. In this paper, we approach to this problem in the following way.

Let G be an abelian p -group. Then G has a subnormal series

$$\langle e \rangle = G_o < G_1 < \cdots < G_n = G$$

such that each factor group G_i/G_{i-1} is a cyclic group of order p . Existence of this composition series allows us to define *long presentation* (see section 2) of G , and moreover, there is an *enumeration* (see section 2) in the system of long generators. We shall inductively compute the complete set of primitive central idempotents of $\mathbb{Q}[G]$ using that *long presentation*.

A remarkable thing is that as a consequence of this inductive process, every primitive central idempotents of $\mathbb{Q}[G]$ can be expressed in product form. Moreover, for a cyclic group of order p^n , n a positive integer, in terms of characters the expression of each primitive central idempotent of complex group algebra has p^n terms, and such a primitive central idempotent factors into n factors, each factor containing p terms. So each primitive central idempotent has an expression containing pn terms, and therefore over \mathbb{Q} this number is less than or equal to pn .

It is an well known fact that Wedderburn decomposition of rational group algebra of a finite abelian group is direct sum of cyclotomic fields. The Classical theory says that the coefficient of cyclotomic field $\mathbb{Q}(\zeta_{p^r})$, where ζ_{p^r} is a primitive p^r th root of unity, appearing in the Wedderburn decomposition of $\mathbb{Q}[G]$ is equal to the number of subgroups of G with factor groups isomorphic to cyclic group of order p^r . We shall explicitly compute those coefficients.

We briefly describe the organization of the paper. In section 2, we shall define *short and long presentations* of an abelian p -group. In section 3, we shall define PCI-diagrams of an abelian p -group. In section 4, we shall give an explicit expression of primitive central idempotents of an abelian p -group over an algebraically closed field using *long presentation*. In section 5, we shall give an explicit expression of primitive central idempotents of rational group algebra of a finite abelian p -group using *long presentation*. In section 6, we shall compute coefficients of cyclotomic fields appearing in the Wedderburn decomposition of rational group algebra of a finite abelian p -group.

We use the following notations. Throughout this paper we assume that G is a finite group. We denote the order of G by $|G|$. By F we mean a field with characteristic does not divide $|G|$. By $F[G]$, we mean the group algebra of G over F . For $X \subset G$, $\langle X \rangle$ denotes the subgroup generated by X . For $H \leq G$, \hat{H} denotes the idempotent $\frac{1}{|H|} \sum_{h \in H} h$ of $\mathbb{Q}[G]$. We denote cyclic group of order n by C_n . For a positive integer n , ζ_n denotes a complex primitive n th root of unity and $\mathbb{Q}(\zeta_n)$ denotes n th cyclotomic field over \mathbb{Q} . By p we always mean a prime number. Throughout this paper we use e_X for $\frac{1+X+\dots+X^{p-1}}{p}$, where X is an indeterminate, and e'_X for $1 - e_X$.

2. SHORT AND LONG PRESENTATIONS OF AN ABELIAN p -GROUP

Let G be an abelian p -group of order p^N . It is known that abelian groups of order p^N are parametrized by partitions of N . Let $N = s_1 + s_2 + \dots + s_m$ be a partition of N , and let r_i is a divisor of s_i , so that after re-indexing $r_1 > r_2 > \dots > r_m \geq 1$, and for each i , let $s_i = r_i l_i$. To this partition of N , we associate the abelian p -group

$$(2.1) \quad G = \prod_{i=1}^m \prod_{j=1}^{l_i} C_{p^{r_i, j}},$$

where $C_{p^{r_i, j}}$ denotes the j th factor of the *homo-cyclic component* of exponent p^{r_i} . We define a *short presentation* of $C_{p^{r_i, j}}$ as $\langle y_{(r_i, j)} | y_{(r_i, j)}^{p^{r_i}} = e \rangle$, and the generator $y_{(r_i, j)}$ is called *short generator* of $C_{p^{r_i, j}}$. Therefore a *short presentation* of G is defined by

$$\prod_{i=1}^m \prod_{j=1}^{l_i} \langle y_{(r_i, j)} \mid y_{(r_i, j)}^{p^{r_i}} = e \rangle.$$

Notice that a short presentation contains minimum number of generators. Now we make a refinement of *short presentation*, and use the terminology *long presentation* for that. We use three in-dices to represent a generator in a *long presentation* of G . We define a *long presentation* of $C_{p^{r_i, j}}$ as

$$\begin{aligned} \langle x_{\{(r_i, j), r_i\}}, x_{\{(r_i, j), r_i-1\}}, \dots, x_{\{(r_i, j), 1\}} \mid & x_{\{(r_i, j), r_i\}}^p = x_{\{(r_i, j), r_i-1\}}, \\ & x_{\{(r_i, j), r_i-1\}}^p = x_{\{(r_i, j), r_i-2\}}, \\ & \dots, \\ & x_{\{(r_i, j), 1\}}^p = 1 \rangle. \end{aligned}$$

We call the set $\{x_{\{(r_i, j), r_i\}}, x_{\{(r_i, j), r_i-1\}}, \dots, x_{\{(r_i, j), 1\}}\}$, a *system of long generators* of $C_{p^{r_i, j}}$. Therefore a *long presentation* of G is defined by

$$\begin{aligned} \prod_{i=1}^m \prod_{j=1}^{l_i} \langle x_{\{(r_i, j), r_i\}}, x_{\{(r_i, j), r_i-1\}}, \dots, x_{\{(r_i, j), 1\}} \mid & x_{\{(r_i, j), r_i\}}^p = x_{\{(r_i, j), r_i-1\}}, \\ & x_{\{(r_i, j), r_i-1\}}^p = x_{\{(r_i, j), r_i-2\}}, \\ & \dots, \\ & x_{\{(r_i, j), 1\}}^p = 1, \\ & com \rangle. \end{aligned}$$

We call (s, j) , the place index and a , the power index of the long generator $x_{\{(s, j), a\}}$. An interesting thing is that, there is an enumeration in a system of long generators with respect to the lexicographic order. Note that, every element of G can be expressed uniquely as product of $x_{\{(s, j), a\}}^{\alpha_{\{(s, j), a\}}}$'s, where $0 \leq \alpha_{\{(s, j), a\}} \leq p - 1$.

3. PCI-DIAGRAM OF AN ABELIAN p -GROUP

In this section we define PCI-diagram of an abelian p -group.

Definition 3.1. Let G be an abelian p -group of order p^N . Then G has a subnormal series

$$\{e\} = G_0 < G_1 < \cdots < G_N = G$$

such that $G_i/G_{i-1} = \langle x_i G_{i-1} \rangle$, for some x_i in G_i and is isomorphic to C_p . Let p be an invertible element in F . Let I_{G_i} denotes the complete set of primitive central idempotents of $F[G_i]$, where i runs over the set $\{0, 1, \dots, N\}$. Let e be an element in I_{G_i} , and (η, W) be its associated irreducible F -representation. Suppose that the induced representation $\text{Ind}(\eta, W) \uparrow_{G_{i-1}}^{G_i}$ decomposes into l distinct irreducible F -representations $(\rho_1, V_1), (\rho_2, V_2), \dots, (\rho_l, V_l)$ with multiplicities n_1, n_2, \dots, n_l respectively, i.e.,

$$\text{Ind}(\eta, W) \uparrow_{G_{i-1}}^{G_i} = \bigoplus_{j=1}^l n_j(\rho_j, V_j).$$

For each j , let e_j be the primitive central idempotent associated to the irreducible representation (ρ_j, V_j) . We define the PCI-diagram associated to the above composition series is a graph, whose vertex set is $\cup_{i=0}^N I_{G_i}$, and the vertex e is adjacent to l vertices e_1, e_2, \dots, e_l . We call I_{G_i} as vertex set at the i th level of the PCI-diagram.

Remark 1. The definition of PCI-diagram can be generalized for finite solvable groups, as a finite solvable group always has a subnormal series with successive quotient groups are cyclic groups of prime order.

4. PRIMITIVE CENTRAL IDEMPOTENTS OF AN ABELIAN GROUP OVER AN ALGEBRAICALLY CLOSED FIELD:

In this section, we compute primitive central idempotents of an abelian group over an algebraically closed field. But to compute primitive central idempotents of an abelian group over an algebraically closed field it is sufficient to compute primitive central idempotents of a cyclic group of prime power order. In this case, we shall see that the primitive central idempotents factor nicely.

Theorem 4.1. Let G be C_{p^n} , with the long presentation:

$$G = \langle x_1, x_2, \dots, x_n \mid x_1^p = 1, x_2^p = x_1, \dots, x_n^p = x_{n-1} \rangle.$$

Let F be an algebraically closed field with characteristic 0. Let ζ_n be a p^n th root of unity in F . Then every primitive central idempotent of $F[G]$ is of the form:

$$e_{\zeta_1 x_1} e_{\zeta_2 x_2} \cdots e_{\zeta_n x_n},$$

where ζ_i 's are p^i -th power roots of unity in F defined by $\zeta_n^p = \zeta_{n-1}, \dots, \zeta_2^p = \zeta_1$.

Proof. Every element of G can be expressed uniquely as $x_1^{i_1} x_2^{i_2} \dots x_n^{i_n}$ where i_j 's are running over the set $\{0, 1, \dots, p-1\}$. Let ρ be an F -irreducible representation of G , then $\rho(x_j)$ is a p^j -th root of unity, ζ_j (say) and then $\rho(x_j^p) = \{\rho(x_j)\}^p = \zeta_j^p = \zeta_{j-1}$, $j = 1, 2, \dots, n$. Then the primitive central idempotent corresponding to ρ is:

$$\begin{aligned} e_\rho &= \frac{1}{p^n} \sum_{g \in G} \rho(g^{-1})g \\ &= \frac{1}{p^n} \left\{ \sum_{i_1=0}^{p-1} \sum_{i_2=0}^{p-1} \dots \sum_{i_{n-1}=0}^{p-1} \sum_{i_n=0}^{p-1} \rho\{(x_1^{i_1} x_2^{i_2} \dots x_n^{i_n})^{-1}\} (x_1^{i_1} x_2^{i_2} \dots x_n^{i_n}) \right\} \end{aligned}$$

This implies that

$$\begin{aligned} e_\rho &= \frac{1}{p^{n-1}} \left\{ \sum_{i_1=0}^{p-1} \sum_{i_2=0}^{p-1} \dots \sum_{i_{n-1}=0}^{p-1} \rho(x_1^{i_1} x_2^{i_2} \dots x_{n-1}^{i_{n-1}})^{-1} (x_1^{i_1} x_2^{i_2} \dots x_{n-1}^{i_{n-1}}) \right\} \\ &\quad \left\{ \frac{1}{p} \left(1 + \frac{x_n}{\rho(x_n)} + \dots + \frac{x_n^{p-1}}{\rho(x_n)^{p-1}} \right) \right\} \\ &= \frac{1}{p^{n-1}} \left\{ \sum_{i_1=0}^{p-1} \sum_{i_2=0}^{p-1} \dots \sum_{i_{n-1}=0}^{p-1} \rho(x_1^{i_1} x_2^{i_2} \dots x_{n-1}^{i_{n-1}})^{-1} (x_1^{i_1} x_2^{i_2} \dots x_{n-1}^{i_{n-1}}) \right\} e_{\zeta_n^{-1} x_n}. \end{aligned}$$

Similarly, if we keep continuing this process, finally we get:

$$e_\rho = e_{\zeta_1^{-1} x_1} e_{\zeta_2^{-1} x_2} \dots e_{\zeta_n^{-1} x_n},$$

where $\zeta_n^p = \zeta_{n-1}$, \dots , $\zeta_2^p = \zeta_1$. Replacing x_i by x_i^{-1} we get:

$$e_\rho = e_{\zeta_1^{-1} x_1^{-1}} e_{\zeta_2^{-1} x_2^{-1}} \dots e_{\zeta_n^{-1} x_n^{-1}}.$$

This completes the proof of the theorem. □

Theorem 4.2. Let G be C_{p^n} , with the long presentation:

$$G = \langle x_1, x_2, \dots, x_n \mid x_1^p = 1, x_2^p = x_1, \dots, x_n^p = x_{n-1} \rangle.$$

Let F be an algebraically closed field with characteristic 0. Let H be the unique subgroup of index p of G with the long presentation:

$$H = \langle x_1, x_2, \dots, x_{n-1} \mid x_1^p = 1, x_2^p = x_1, \dots, x_{n-1}^p = x_{n-2} \rangle.$$

Let η be an F -irreducible representation of H and let e_η be its corresponding primitive central idempotent. Let $e_\eta = e_{\zeta_1 x_1} e_{\zeta_2 x_2} \dots e_{\zeta_{n-1} x_{n-1}}$ with $\zeta_{n-1}^p = \zeta_{n-2}$, \dots , $\zeta_2^p = \zeta_1$. Then:

- (1) η extends to p mutually inequivalent F -irreducible representations $\rho_0, \rho_1, \dots, \rho_{p-1}$ of G .

- (2) The primitive central idempotents associated to ρ_i 's are $e_\eta e_{\epsilon^i \zeta_n x_n}$, where i runs over the set $\{0, 1, \dots, p-1\}$, ζ_n is a fixed p -th root of ζ_{n-1} and ϵ is a primitive p -th root of unity in F .

Proof. Since every F -irreducible representation of G is 1-dimensional, then clearly η extends to an F -irreducible representation of G . Suppose that η extends to ρ , this implies that $\{\rho(x_n)\}^p = \rho(x_n^p) = \eta(x_n^p) = \eta(x_{n-1}) = \zeta_{n-1}$. Therefore $\rho(x_n)$ is equal to $\epsilon^i \zeta_n$, where ϵ is a primitive p th root of unity, and ζ_n is a fixed p -th root of ζ_{n-1} , and i runs over the set $\{0, 1, \dots, p-1\}$. So η extends precisely p distinct ways. This completes the first part of the theorem.

Let $\rho_0, \rho_1, \dots, \rho_{p-1}$ be p extensions of η , and $e_{\rho_0}, e_{\rho_1}, \dots, e_{\rho_{p-1}}$ be their corresponding primitive central idempotents of $F[G]$. Then for each $i \in \{0, 1, \dots, p-1\}$,

$$e_{\rho_i} = \frac{1}{p^n} \sum_{g \in G} \rho_i(g^{-1})g.$$

Again the previous expression can be written as:

$$e_{\rho_i} = \frac{1}{p^n} \left[\sum_{h \in H} \rho_i(h^{-1})h + \sum_{h \in H} \{\rho_i(h^{-1})h\} \{\rho_i(x_n^{-1})x_n\} + \dots + \sum_{h \in H} \{\rho_i(h^{-1})h\} \{\rho_i(x_n^{-(p-1)})x_n^{p-1}\} \right]$$

Therefore,

$$\begin{aligned} e_{\rho_i} &= \left\{ \frac{1}{p^n} \sum_{h \in H} \rho_i(h^{-1})h \right\} \left\{ 1 + \frac{x_n}{\rho_i(x_n)} + \dots + \frac{x_n^{p-1}}{\rho_i(x_n^{p-1})} \right\} \\ &= \frac{e_\eta}{p} \left\{ 1 + \frac{x_n}{\rho_i(x_n)} + \dots + \frac{x_n^{p-1}}{\rho_i(x_n^{p-1})} \right\} \\ &= \frac{e_\eta}{p} \left\{ 1 + \frac{x_n}{\rho_i(x_n)} + \dots + \frac{x_n^{p-1}}{\rho_i(x_n^{p-1})} \right\} \\ &= e_\eta e_{\epsilon^{-i} \zeta_n^{-1} x_n}, \end{aligned}$$

where ζ_n is a fixed p th root of ζ_{n-1} and $\epsilon \neq 1$ is a p -th root of unity in F . Replacing x_n by x_n^{-1} we get $e_{\rho_i} = e_\eta e_{\epsilon^{-i} \zeta_n^{-1} x_n^{-1}}$. This proves the second statement of the theorem. \square

5. PRIMITIVE CENTRAL IDEMPOTENTS OF AN ABELIAN p -GROUP OVER \mathbb{Q}

In this section, we compute the primitive central idempotents of an abelian p -group algebra over \mathbb{Q} . We shall proceed inductively. Let G be an abelian p -group. Then G always have a composition series. For computing primitive central idempotents of $\mathbb{Q}[G]$ inductively we choose a composition series of G in such a way that i is increasing as well as j is decreasing in the equation (2.1).

5.1. Rational Group Algebra of a Cyclic Group. If F and E are fields, $F \subseteq E$, we denote by $[E : F]$ the degree of the field extension; that is, the dimension of E as a vector space over F .

An element $\zeta \in \mathbb{C}$ is said to be a root of unity if $\zeta^n = 1$ for some $n \geq 1$. A root of unity ζ is said to be primitive m th root of unity if m is the smallest positive integer with the property that $\zeta^m = 1$. The m th cyclotomic polynomial is

$$\Phi_m(x) = \prod_{\zeta} (x - \zeta),$$

where the product has taken over all primitive m th roots of unity. It is well known that $\Phi_m(x)$ has coefficients in \mathbb{Q} and this polynomial is irreducible over \mathbb{Q} . The degree of the polynomial $\Phi_m(x)$ is $\phi(m)$, where ϕ is the Euler ϕ function; that is, $\phi(m)$ is the number of integers k , $1 \leq k \leq m$, which are relatively prime to m .

Let ζ_m be a primitive m th root of unity in \mathbb{C} . Then the mapping

$$\frac{\mathbb{Q}[X]}{\Phi_m(X)} \longrightarrow \mathbb{Q}(\zeta_m)$$

defined by $x + (\Phi_m(x)) \mapsto \zeta_m$ is an isomorphism and so

$$\mathbb{Q}(\zeta_m) \cong \frac{\mathbb{Q}[x]}{(\Phi_m(x))}$$

is a field extension of \mathbb{Q} of degree $\phi(m)$ known as a cyclotomic field. Since for $n \geq 1$, the polynomial $x^n - 1$ factors

$$x^n - 1 = \prod_{m|n} \Phi_m(x)$$

the rational group algebra of the cyclic group C_n of order n is

$$\mathbb{Q}[C_n] \cong \frac{\mathbb{Q}[x]}{(x^n - 1)} \cong \bigoplus_{m|n} \frac{\mathbb{Q}[x]}{\Phi_m(x)} \cong \bigoplus_{m|n} \mathbb{Q}(\zeta_m).$$

5.2. Primitive Central Idempotents of C_{p^n} over \mathbb{Q} . The following proposition gives an explicit description of the complete set of primitive central idempotents of C_{p^n} over \mathbb{Q} using long presentation.

Proposition 5.1. *Let G be C_{p^n} , where n is a positive integer. Then G has the long presentation:*

$$G = \langle x_1, x_2, \dots, x_n \mid x_1^p = 1, x_2^p = x_1, \dots, x_n^p = x_{n-1} \rangle.$$

Let $e_0 = e_{x_1} e_{x_2} \dots e_{x_n}$ and $e_i = e_{x_1} e_{x_2} \dots e_{x_{i-1}} e'_{x_i}$, where $i \in \{1, 2, \dots, n\}$. Then the set $\{e_0, e_1, \dots, e_n\}$ is the complete set of primitive central idempotents of $\mathbb{Q}[G]$.

Proof. Since the rational group algebra $\mathbb{Q}[G] \cong \bigoplus_{i=0}^n \mathbb{Q}(\zeta_{p^i})$, then $\mathbb{Q}[G]$ contains precisely $n + 1$ primitive central idempotents. One can show that $(e_{x_1} e_{x_2} \dots e_{x_i})(e_{x_1} e_{x_2} \dots e_{x_j}) = (e_{x_1} e_{x_2} \dots e_{x_j})$, for $1 \leq i \leq j$, and therefore e_i 's are idempotents. Now we verify orthogonality condition. For $i \geq 1$, $e_0 e_i = (e_{x_1} e_{x_2} \dots e_{x_n}) e_i = (e_{x_1} e_{x_2} \dots e_{x_n}) \{(e_{x_1} e_{x_2} \dots e_{x_{i-1}}) -$

$(e_{x_1}e_{x_2}\dots e_{x_i})\} = 0$. Hence e_0 is orthogonal to e_i . Now assume that $1 \leq i \leq j$, then

$$\begin{aligned} e_i e_j &= (e_{x_1}e_{x_2}\dots e'_{x_i})(e_{x_1}e_{x_2}\dots e'_{x_j}) \\ &= \{e_{x_1}e_{x_2}\dots e_{x_{i-1}}(1 - e_{x_i})\}\{e_{x_1}e_{x_2}\dots e_{x_{j-1}}(1 - e_{x_j})\} \\ &= 0. \end{aligned}$$

It is easy to see that $\sum_{i=0}^n e_i = 1$. It follows that e_0, e_1, \dots, e_n are $n+1$ pairwise orthogonal central idempotents whose sum is 1, hence this is the complete set of primitive central idempotents of $\mathbb{Q}[G]$. This completes the proof of the proposition. \square

5.3. PCI-diagram of an Abelian p -Group over \mathbb{Q} . We state four rules by which one can inductively construct primitive central idempotents and draw PCI-diagram of an abelian p -group over \mathbb{Q} .

Rule 0: Each non trivial primitive central idempotent at any stage can be expressed in a product form and contains exactly one e'_z as a factor, where z is a generator of the chosen long presentation of G .

Proof of the Rule 0: Let e be a non trivial primitive central idempotent at the l th stage of PCI- diagram, i.e., e is a non trivial primitive central idempotent of $\mathbb{Q}[G_l]$. Without loss generality one can assume that G_l is equal to G . By Maschake's theorem and commutativity, the semisimple artinian ring $\mathbb{Q}[G]$ is direct sum of fields. In particular, $\mathbb{Q}[G]e$ is a field and contains the finite subgroup $Ge = \{ge | g \in G\}$ which is necessarily cyclic, say of order p^n , $n \geq 0$. Let $K = \{g \in G | ge = e\}$. Then

$$Ge \cong \frac{G}{K} = \langle \bar{x}_1, \bar{x}_2, \dots, \bar{x}_n \mid \bar{x}_1^p = 1, \bar{x}_2^p = \bar{x}_1, \dots, \bar{x}_n^p = \bar{x}_{n-1} \rangle,$$

where \bar{x}_i denotes the image of x_i in the factor group G/K . Again by lemma 5.2, the group algebra $\mathbb{Q}[G] = \mathbb{Q}[G]\hat{K} \oplus \mathbb{Q}[G](1 - \hat{K})$ and because $\hat{K}e = e$, it follows that $\mathbb{Q}[G]e = \mathbb{Q}[G]\hat{K}e$ is actually simple component of $\mathbb{Q}[G]\hat{K}$. Thus e is also primitive central idempotent of $\mathbb{Q}[G]\hat{K} \cong \mathbb{Q}[\frac{G}{K}]$.

Let $\phi : \mathbb{Q}[G] \rightarrow \mathbb{Q}[\frac{G}{K}]$ be the homomorphism induced by the natural group epimorphism $G \rightarrow \frac{G}{K}$ and with the kernel $\mathbb{Q}[G](1 - \hat{K})$. Recall that $e = \hat{K}e \mapsto \phi(e)$ under the isomorphism $\phi : \mathbb{Q}[G]\hat{K} \rightarrow \mathbb{Q}[\frac{G}{K}]$. Thus $\phi(e)$ is a primitive central idempotent in $\mathbb{Q}[\frac{G}{K}]$. Writing $e = \sum_{g \in G} e(g)g$, $e(g) \in \mathbb{Q}$, we note that some $e(g) \neq \frac{1}{|G|}$, because e is a non trivial primitive central idempotent of $\mathbb{Q}[G]$. Since $ke = e$ for any $k \in K$, it follows that $e(g) = e(kg)$ for any $g \in G$ and $k \in K$, so the coefficients of e is constant on cosets of K . Thus

$$e = \sum_{i=0}^{p^n-1} \alpha_i \widehat{K} x_n^i,$$

with each $\alpha_i \in \mathbb{Q}$ and, for some i , $\frac{\alpha_i}{|\widehat{K}|} = \frac{1}{|G|}$; that is, for some i , $\alpha_i \neq \frac{1}{|\widehat{K}|}$. Since

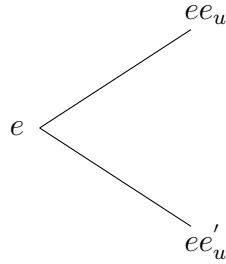
$$\phi(e) = \sum_{i=0}^{p^n-1} \alpha_i \bar{x}_n^i,$$

it must be that $\phi(e) \neq \frac{\widehat{G}}{K}$. hence by the lemma 7.1 we get

$$\phi(e) = e_i = \{(e_{\bar{x}_1} e_{\bar{x}_2} \dots e_{x_{i-1}}) - (e_{\bar{x}_1} e_{\bar{x}_2} \dots e_{\bar{x}_i})\},$$

for some i , $1 \leq i \leq n$. Then $e = \widehat{K}\{(e_{x_1} e_{x_2} \dots e_{x_{i-1}}) - (e_{x_1} e_{x_2} \dots e_{x_i})\}$, which implies that $e = \{\widehat{K}(e_{x_1} e_{x_2} \dots e_{x_{i-1}})\}(1 - e_{x_i})$, for some i , $1 \leq i \leq n$. Again, \widehat{K} can be expressed product of certain number of e_x , where $x \in G$. Hence each non trivial primitive central idempotent at any stage of PCI- diagram can be expressed in a product form and contains precisely one e'_z as a factor, where z is a generator of the chosen long presentation of G . This completes the proof of the theorem.

Rule 1: Let e be the trivial primitive central idempotent in the l th stage of the PCI- diagram. Let u be the new generator introduced in the $l+1$ st stage of chosen long presentation of G . Then e is adjacent to precisely two vertices ee_u and ee'_u in the $l+1$ st stage of PCI- diagram. In term of picture this rule is:



Proof of the Rule 1: First observe that e is central idempotent in $\mathbb{Q}[G_{l+1}]$. So $\mathbb{Q}[G_{l+1}]e$ is an ideal in $\mathbb{Q}[G_{l+1}]$, which is semisimple component corresponding to the induced representation of irreducible representation associated to e from G_l to G_{l+1} . Now the ideal $\mathbb{Q}[G_{l+1}]e$ is direct sum of minimal ideals in $\mathbb{Q}[G_{l+1}]$, in other words direct sum of simple rings. One can see that $\mathbb{Q}[G_{l+1}]ee_u$ is one simple component of $\mathbb{Q}[G_{l+1}]e$. Since $\mathbb{Q}[G_{l+1}]e$ is direct sum of two simple components, then $\mathbb{Q}[G_{l+1}]ee'_u$ is another simple component of $\mathbb{Q}[G_{l+1}]e$. Hence e is adjacent to the precisely two vertices ee_u and ee'_u at the $(l+1)$ st stage of the PCI- diagram.

Rule 2: Let e be a non trivial primitive central idempotent in the l th stage of PCI- diagram. Then e contains precisely one e'_z as a factor, where z is a generator of the chosen long presentation. Let u be the long generator introduced in the $l + 1$ st stage of PCI- diagram such that $z = u^{p^s}$, for some +ve integer s . Then e is adjacent to itself in the $l + 1$ st stage of the PCI- diagram. In term of picture this rule is:

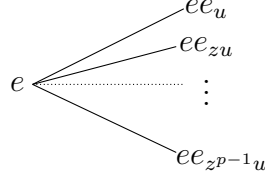
$$e \text{ ————— } e$$

Proof of the Rule 2: Since e is a non trivial primitive central idempotent at the l th stage of the PCI- diagram, then e is a non trivial primitive central idempotent of the group algebra $\mathbb{Q}[G_l]$. By previous theorem, e is pull back of primitive central idempotent of cyclic quotient G/K , which is isomorphic to C_{p^n} (say), for some $n \geq 1$, infact it is pull back of unique faithfull irreducible representation of G/K . Again, since e contains precisely one e'_z , where z is a generator of the chosen long presentation of G , then e is pull back of primitive central idempotent $e'_{\bar{z}}$ of G_l/K , where \bar{z} si equal to the coset zK . Notice that \bar{z} is the first generator in the long presentation of G_l/K .

Now, as u is the generator inserted in the $(l + 1)$ st stage of the chosen long presentation of G , then $G_{l+1} = \langle G_l, u \rangle$. Again, since $z = u^{p^s}$, for some +ve integer s , then G_{l+1}/K is isomorphic to $C_{p^{n+1}}$. Again notice that \bar{z} is the first generator of the long presentation of G_{l+1}/K . Thus e is also pull back of primitive central idempotent $e'_{\bar{z}}$ of G_{l+1}/K . Therefore $\mathbb{Q}[G_{l+1}]e$ is minimal ideal of $\mathbb{Q}[G_{l+1}]$. Hence e is adjacent to itself at the $(l + 1)$ st stage of PCI- diagram.

Rule 3: Let e be a non trivial primitive central idempotent in the l th stage of PCI- diagram. Then e contains precisely one e'_z as a factor, where z is a generator of the chosen long presentation. Let u be the long generator introduced in the $l + 1$ st stage of PCI- diagram such that $z \neq u^{p^s}$, for any +ve integer s . Then e is adjacent to precisely p vertices $ee_u, ee_{zu}, \dots, ee_{z^{p-1}u}$ in the $l + 1$ st stage of the PCI- diagram.

In term of picture this rule is:

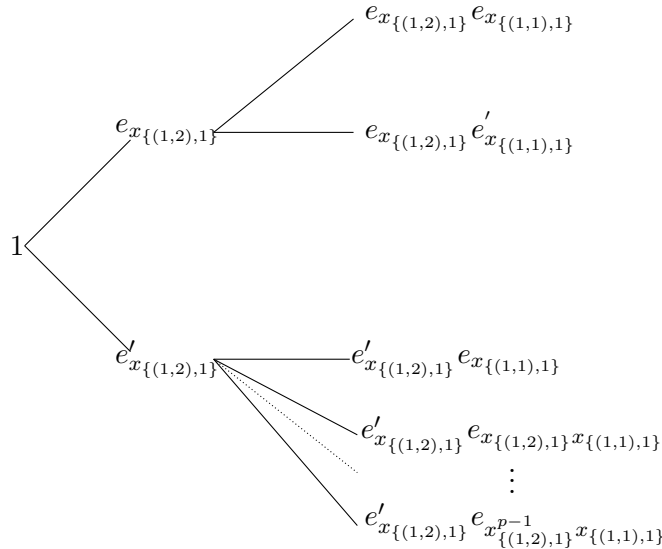


Proof of the Rule 3: By the theorem(5.2), as e is a nontrivial primitive central idempotent of $\mathbb{Q}[G_l]$, then e is lift of primitive central idempotent of a cyclic quotient G/K , $K \neq G_l$, which is isomorphic to C_{p^n} (say), where n is a positive integer. Since e contains e'_z as a factor, then first long generator of the cyclic quotient G/K is equal to \bar{z} , where \bar{z} denotes the coset zK . It is quite clear that e is equal to $\widehat{K}e'_z$. By hypothesis, $z \neq u^{p^s}$, for any positive integer s , then the subgroups: $\langle K, u \rangle, \langle K, zu \rangle, \dots, \langle K, z^{p-1}u \rangle$ are all distinct subgroups of G_{l+1} . One can observe that, for each $i \in \{0, 1, \dots, p-1\}$, the quotient group $G_{l+1}/\langle K, z^i u \rangle$ is isomorphic to G_l/K . So, for each i , the first generator of the cyclic quotient $G_{l+1}/\langle K, z^i u \rangle$ is \bar{z} , where \bar{z} denotes the coset $z\langle K, z^i u \rangle$. Therefore, for each i , lift of e'_z is equal to $\widehat{\langle K, z^i u \rangle}e'_z = ee_{z^i u}$. Hence the set $\{e_{z^i u} \mid i = 0, 1, \dots, p-1\}$ are p distinct primitive central idempotents of $\mathbb{Q}[G_{l+1}]$. It is clear that each $\mathbb{Q}[G_{l+1}]ee_{z^i u}$ belongs to $\mathbb{Q}[G_{l+1}]e$. One can show that the ideal $\mathbb{Q}[G_{l+1}]e$ is direct sum of p minimal ideals of $\mathbb{Q}[G_{l+1}]$ and then $\mathbb{Q}[G_{l+1}]e = \bigoplus_{i=0}^{p-1} \mathbb{Q}[G_{l+1}]ee_{z^i u}$.

Example 1. Let

$$G = C_p \times C_p = \langle x_{\{(1,2),1\}}, x_{\{(1,1),1\}} \mid x_{\{(1,2),1\}}^p = 1, x_{\{(1,1),1\}}^p = 1, com \rangle.$$

The associated PCI- diagram is



6. WEDDERBURN DECOMPOSITION OF RATIONAL GROUP ALGEBRA OF AN ABELIAN p -GROUP

In this section we compute the coefficients of cyclotomic fields, which are appearing in the Wedderburn decomposition of rational group algebra of an abelian p -group. Let us fix some notations for that.

Let $G = \prod_r G_r$, where G_r is a product of a_r copies of cyclic groups of order p^r , and of exponent p^n . Let $b_r = a_r + a_{r+1} + \cdots + a_n$ and $c_r = a_1 + 2a_2 + \cdots + (r-1)a_{r-1}$. Let $B_r = \prod_{s \leq r} G_s$ and then $G = B_r \times \prod_{s > r} G_s$. Let $\Omega^r(G) = \{g \in G \mid g^{p^r} = 1\}$, then $\Omega^r(G) = B_r \times$ product of b_r copies of cyclic groups of order p^r . Let H_r be the product of b_r copies of cyclic groups of order p^r . Then $\Omega^r(G) = B_r \times H_r$. Let $E_r(G) = \{g \in G \mid o(g) = p^r\}$, then $|E_r(G)| = |\Omega^r(G)| - |\Omega^{r-1}(G)|$. Therefore the number of cyclic subgroups of G isomorphic to C_{p^r} is equal to $|E_r(G)|/\phi(p^r)$, where ϕ denotes Euler's phi function. The next proposition says that the number $|E_r(G)|/\phi(p^r)$ is same as the number of subgroups of G with factor groups isomorphic to C_{p^r} .

Proposition 6.1. *The number of subgroups of G with factor groups isomorphic to C_{p^r} is equal to the number of cyclic subgroups of G isomorphic to C_{p^r} , and therefore this number is same as $|E_r(G)|/\phi(p^r)$.*

Proof. Let H be a subgroup of G , such that G/H isomorphic to C_{p^r} . We consider $\tilde{H} = \{\chi \in \hat{G} \mid \chi = 1 \text{ on } H\}$, then \tilde{H} is a subgroup of \hat{G} . Let ψ be an isomorphism from \hat{G} onto \hat{G} , and assume that $\psi(\tilde{H})$ is equal to K (say). It is easy to show that \tilde{H} is isomorphic to C_{p^r} , and hence K is isomorphic to C_{p^r} .

Suppose that H_1, H_2 are two distinct subgroups of G such that factor groups are isomorphic to C_{p^r} , and then there exists an element $h \in H_1 - H_2$, and therefore $\tilde{H}_1 \neq \tilde{H}_2$. So $\psi\tilde{H}_1 \neq \psi\tilde{H}_2$. So the number of subgroups of G with factor groups are isomorphic to C_{p^r} is equal to the number of subgroups G isomorphic to C_{p^r} , and hence this number is equal to $|E_r(G)|/\phi(p^r)$. \square

Theorem 6.2. *Let G be an abelian p -group, of exponent p^n . For $r \leq n$, the coefficient of $\mathbb{Q}(\zeta_{p^r})$ in the Wedderburn decomposition of $\mathbb{Q}[G]$ is a polynomial in p . In fact it is equal to $p^{c_r+(r-1)b_r-1} \left(\frac{p^{b_r}-1}{p-1} \right)$.*

Proof. By the theorem (see), the coefficient of $\mathbb{Q}(\zeta_{p^r})$ in the Wedderburn decomposition of $\mathbb{Q}[G]$ is equal to $\frac{|E_r(G)|}{\phi(p^r)}$, where ϕ denotes Euler's phi function. But $|E_r(G)| = |B_r||E_r(H_r)| = p^{c_r}(p^{b_r} - p^{(r-1)b_r}) = p^{c_r+(r-1)b_r}(p^{b_r} - 1)$. Thus the coefficient of $\mathbb{Q}(\zeta_{p^r})$ in the Wedderburn decomposition of $\mathbb{Q}[G]$ is equal to $p^{c_r+(r-1)b_r}(p^{b_r} - 1)/(p^r - p^{r-1}) = p^{c_r+(r-1)(b_r-1)} \left(\frac{p^{b_r}-1}{p-1} \right)$. \square

Remark 2. By the above theorem the coefficient of $\mathbb{Q}(\zeta_{p^r})$ in the Wedderburn decomposition of $\mathbb{Q}[G]$ is equal to $p^{c_r+(r-1)(b_r-1)}\{1 + p + \dots + p^{(b_r-1)}\}$. One can observe that first part of this polynomial is power of p , on the other hand the second part is coprime to p .

REFERENCES

- [1] Ayoub, R. G., Ayoub, C. (1969). *On the group rings of a finite abelian group.* Bull. Austral. Math. Soc. Vol. 1: 245-261.
- [2] Goodaire, E. G., Jespers, E., Milies, C. P. (1996). *Alternative Loop Rings.* Math. Studies Vol. 184. North Holland.
- [3] Jespers, E., Leal, G., Paques, E. (2003). *Central idempotents in rational the group algebras of a finite nilpotent groups.* J. Algebra. Appl. Vol. 2: 57-62.